UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,079	02/06/2004	Shehzad T. Merchant	02453.0019.NPUS00	7139

27194 7590 10/05/2009

HOWREY LLP-CA
C/O IP DOCKETING DEPARTMENT
2941 FAIRVIEW PARK DRIVE, SUITE 200
FALLS CHURCH, VA 22042-2924

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
10/05/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/774,079	MERCHANT ET AL.	
	Examiner	Art Unit	
	JEFFREY D. POPHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 July 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 1-51 are pending.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/28/2009 has been entered.

Response to Arguments

2. Applicant's arguments with respect to claims 1-45 and 48-51 have been considered but are moot in view of the new ground(s) of rejection.

Regarding claims 46-47, however, Applicant argues that "the additional limitation require location-based re-authentication of the mobile upon a handoff from one access point to another." No such re-authentication need take place however. As claim 46 stands, for example, "the mobile client is associated with the newly located access point upon authenticating the identity of the mobile client and determining, by comparing updated location information...". As one can see, this authentication can occur at any point prior to associating with the newly located access point, only the determining aspect of this limitation being

performed using updated information. Therefore, claims 46 and 47 do not require re-authentication.

Specification

3. The attempt to incorporate subject matter into this application by reference to Howrey Docket Nos. 02453.0020.NPUS00 and 02453.0021.NPUS00 is ineffective because the application numbers are missing. The correct application numbers should be added in place of "To Be Determined", such that the application is clearly identified. Alternatively, if the applications have already been patented, patent numbers could be used instead of application numbers.

Claim Objections

4. Claims 15, 29, and 47 are objected to because of the following informalities:

- Claim 15 recites "wherein the user capable of connecting to the network through the access point". It appears as though this should read "wherein the user station is capable of connecting to the network through the access point" since there has been no user set forth in the claims, but rather a user station that is connected to a network switch through an access point.
- Claim 29 recites "a user station that is a wired device for directly connecting one of the ports of the network switch" which should

apparently read "a user station that is a wired device for directly connecting to one of the ports of the network switch".

- Claim 47 recites "wherein the second associating means associates the mobile client with the newly located access point upon authenticating the identity of the mobile client...". It is unclear what entity is performing this authentication, since the second associating means associates the client, but no entity is stated as authenticating the identity of the client. Since the authenticating means of claim 39 is the only entity that performs any authentication, the authenticating means of claim 39 have been construed as that which performs the authentication referred to in claim 47.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-9 and 39-48 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites "during said roaming, when signal quality from a current access point in communication with the mobile client deteriorates sufficiently, locating another access point". It is unclear when, precisely, the signal quality

will deteriorate "sufficiently". While the specification provides for locating an access point upon complete loss of the signal as well as proactive scanning for a stronger signal, it does not define when deterioration of signal quality will be "sufficient". The proactive scanning merely provides for scanning for a stronger signal and then associating with the new access point, which appears as though it could occur at the same signal strength as the client was originally connected to the previous access point, merely associating with another access point upon finding a better signal. Claim 39 has the same issue and is, therefore, rejected for the same reasons. Claims 2-9 and 40-48, depending from claims 1 or 39, are also rejected for the same reasons.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 10, 17-19, 21-24, and 26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 10 is directed to a network system comprising a network, an authenticator, a data structure, an authentication server, and a network manager. None of these entities are inherently physical. A network is a connection of entities. An authenticator is described in the application as being located at a switch or edge device. Therefore, the authenticator can be merely software. A data structure is data by its very basis. An authentication server "can be included as a component

in one or more of the switches" (page 8, lines 28-30). This is also shown in claim 20. The only interpretation one can make of this is that an authentication server need not be a physical entity, but may be logical (e.g. program code). Therefore, the authentication server (and broader server) need not include physical components. Furthermore, a server is generally defined as being a device or a program. A network manager is described in the specification, such that "The network manager 20 can be a server running an application" (page 6, lines 14-15). Therefore, the interpretation taken for a network manager is equivalent to that of a server. All of the entities of claim 10 could be hardware, software/logical, or a combination thereof. Therefore, claim 10 fails to fall in one of the statutory categories of invention, since it is not a process, apparatus, article of manufacture, or composition of matter. Claims 11-16, 20, and 25 provide physical elements (edge devices, client devices, and network switches) and are, therefore, statutory. Claims 17-19, 21-24, and 26, however, do not fix the issue, and are rejected for the same reasons as claim 10.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 2, 4-6, 9, 39, 40-42, and 45-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart (U.S. Patent 6,732,176) in view of Choi (U.S. Patent Application Publication 2004/0224690).

Regarding Claim 1,

Stewart discloses a method of controlling access to a network, comprising:

Requesting an identity from a mobile client attempting to connect to the network (Column 10, line 64 to Column 11, line 16);

Receiving the identity (Column 10, line 64 to Column 11, line 16);

Associating location information corresponding to the client with the identity (Column 11, lines 17-53);

Authenticating the identity (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; and Column 18, lines 1-25);

Comparing the location information against a policy designating locations, if any, at which the client is permitted to connect to the network (Column 11, lines 28-53; and Column 16, lines 38-64; determining access levels based on location);

Deciding whether to grant or deny the client access to the network based on the authenticity of the identity and the comparison of the location information (Column 11, lines 28-53; Column 12, lines 47-63; and Column 16, lines 15-55; granting

differing levels of access based on identification information as well as geographic information);

When access is granted, permitting roaming of the mobile client within the network (Column 10, lines 25-37; and Column 14, line 57 to Column 15, line 15; the users are allowed to roam and/or walk around, connecting to different APs, for example);

During the roaming, locating another access point (Column 10, lines 25-37; Column 11, lines 28-53; Column 14, lines 21-39; and Column 16, lines 38-64; for example, walking around the airport and finding another AP in the airport (e.g. an AP in an Admiral's Club or at the airline gate));

When another access point is located, associating the mobile client with the newly located access point and allowing the client to continue to access the network upon determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network (Column 10, lines 25-37; Column 11, lines 28-53; Column 14, lines 21-39; and Column 16, lines 38-64; providing access based on the location that the client is currently located, such that the client is provided with a greater access level to more network resources at the Admiral's Club than at the airline gate, for example);

But does not explicitly disclose determining that signal quality from a current access point in communication with the mobile client deteriorates sufficiently.

Choi, however, discloses determining that signal quality from a current access point in communication with the mobile client deteriorates sufficiently and associating the mobile client with a newly located access point (Paragraphs 62-63 and 81-83). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the handoff techniques of Choi into the distributed network access system of Stewart in order to allow the client to determine when signal strength from the present AP has become weak and contact a new AP that has the strongest signal of near APs by using information regarding near APs from the present AP, thereby reducing the time required to find a new AP and, thus, the delay of transmission involved with handoffs, while optimizing the signal strength of the new AP.

Regarding Claim 39,

Claim 39 is a system claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 2,

Stewart as modified by Choi discloses the method of claim 1, in addition, Stewart discloses passing the identity and the location information to an authentication server, wherein the authentication

server performs the steps of authenticating, comparing and deciding (Column 10, line 64 to Column 11, line 16; and Column 14, lines 40-56; the authentication server could be the MIB, for example).

Regarding Claim 4,

Stewart as modified by Choi discloses the method of claim 1, in addition, Stewart discloses that the identity includes information selected from the group consisting of a user name, a user password, a certificate, a MAC address, a shared encryption key, a smart card identifier, and any combination of the foregoing information (Column 10, lines 53-63).

Regarding Claim 40,

Claim 40 is a system claim that corresponds to method claim 4 and is rejected for the same reasons.

Regarding Claim 5,

Stewart as modified by Choi discloses the method of claim 1, in addition, Stewart discloses that the client is a user station capable of connecting to the network through an access point (Column 10, line 64 to Column 11, line 16).

Regarding Claim 41,

Claim 41 is a system claim that corresponds to method claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Stewart as modified by Choi discloses the method of claim 1, in addition, Stewart discloses that the client is a wired device capable of connecting to the network through an Ethernet port (Column 5, lines 2-24; Column 6, lines 40-59; and Column 9, lines 48-64).

Regarding Claim 42,

Claim 42 is a system claim that corresponds to method claim 6 and is rejected for the same reasons.

Regarding Claim 9,

Stewart as modified by Choi discloses the method of claim 1, in addition, Stewart discloses that the location information indicates the location of an edge device for connecting the client to the network (Column 11, lines 17-27).

Regarding Claim 45,

Claim 45 is a system claim that corresponds to method claim 9 and is rejected for the same reasons.

Regarding Claim 46,

Stewart as modified by Choi discloses the method of claim 1, in addition, Stewart discloses that the mobile client is associated with the newly located access point upon authenticating the identity of the mobile client and determining, by comparing updated location information corresponding to the mobile client against a policy, that the mobile client is still authorized to access the network (Column

9, lines 28-47; Column 10, lines 25-37; Column 12, line 30 to Column 13, line 10; Column 14, line 57 to Column 15, line 15; and Column 18, lines 1-25; authentication of the identity of the mobile client is performed at some point prior to an AP allowing requested access; it may be performed at another AP and/or at the current AP by some form of lookup based on the client's identity in order to identify the client to the AP).

Regarding Claim 47,

Claim 47 is a system claim that corresponds to method claim 46 and is rejected for the same reasons.

8. Claims 3, 7, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Choi, further in view of Funk (Funk Software, "Comprehensive RADIUS/AAA Solution for the Global Enterprise", 2/22/2003, pp. 1-6).

Regarding Claim 3,

Stewart as modified by Choi does not explicitly disclose that the authentication server is a RADIUS server.

Funk, however, discloses that the authentication server is a RADIUS server (Pages 1-6). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Choi in order to allow the

system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

Regarding Claim 7,

Stewart as modified by Choi does not explicitly disclose using a mechanism selected form the group comprising TLS, TTLS, MD5, EAP-TLS, and any combination of the foregoing to authenticate the identity.

Funk, however, discloses using a mechanism selected form the group comprising TLS, TTLS, MD5, EAP-TLS, and any combination of the foregoing to authenticate the identity (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Choi in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

Regarding Claim 43,

Stewart as modified by Choi does not explicitly disclose that the authentication means includes an authentication mechanism

selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

Funk, however, discloses that the authentication means includes an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Choi in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

9. Claims 8, 44, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Choi, further in view of Liming (U.S. Patent Application Publication 2002/0055924).

Regarding Claim 8,

Stewart as modified by Choi does not explicitly disclose that the location information indicates the location of a network switch to which the client is attempting to connect.

Liming, however, discloses that the location information indicates the location of a network switch to which the client is

attempting to connect (Paragraph 159). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the location context system of Liming into the distributed network access system of Stewart as modified by Choi in order to allow the system to associate location information with the client even when the other devices cannot provide such location information, thereby extending the system to be able to be used when the client connects directly to a switch and/or when the other devices between the client and switch do not have any means to associate location information with the client.

Regarding Claim 44,

Claim 44 is a system claim that corresponds to method claim 8 and is rejected for the same reasons.

Regarding Claim 48,

Stewart as modified by Choi does not explicitly disclose that the location information indicates the location of a port of a network switch to which the client is attempting to connect.

Liming, however, discloses that the location information indicates the location of a port of a network switch to which the client is attempting to connect (Paragraph 159). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the location context system of Liming into the distributed network access system of Stewart as modified by

Choi in order to allow the system to associate location information with the client even when the other devices cannot provide such location information, thereby extending the system to be able to be used when the client connects directly to a switch and/or when the other devices between the client and switch do not have any means to associate location information with the client.

10. Claims 10, 12-16, 18, 19, 21, 22, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen (U.S. Patent Application Publication 2005/0149443).

Regarding Claim 10,

Stewart discloses a network system comprising:

A network (Figure 1);

An authenticator for requesting an identity from a client and for associating location information corresponding to the client with the identity (Column 10, line 64 to Column 11, line 27);

A data structure, accessible by an authentication server, associating identities of clients with their authorized access locations (Column 7, line 24 to Column 8, line 3; and Column 12, line 55 to Column 13, line 11; Column 15, lines 17-28; and Column 16, lines 38-55; data structure stored on the MIB or other entity, comprising information regarding and associating access levels, locations, identities, providers, etc.);

The authentication server, upon receiving the identity and associated location information from the authenticator, deciding whether to grant or deny the client access to the network by accessing the data structure and determining that the location information corresponding to the client specifies a location that is one of the authorized locations, if any, for the client as maintained in the data structure (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; Column 14, lines 40-56; Column 16, lines 38-55; and Column 18, lines 1-25; the authentication server is any entity accessing the data structure for the purpose of authentication and location-based access; various embodiments of Stewart show the AP, network providers, and/or MIB providing portions of or the entirety of the authentication server);

But does not explicitly disclose a network manager that allows a network administrator to create and update the data structure.

Torvinen, however, discloses a network manager that allows a network administrator to create and update the data structure (Paragraphs 27-28, 42, 45, and 54; showing a management component, for example, that allows the manager or administrator of a particular group or network operator to create and maintain a data structure including a region of interest that is allowed to join the group in order to perform particular actions or acquire particular

data associated with the group). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the conditional group access system of Torvinen into the distributed network access system of Stewart in order to allow various groups to be formed, by network operators and normal users alike, such that groups may be based upon the location of the device, device capabilities, user capabilities or subscriptions, etc., thereby providing additional beneficial services to users by allowing them to communicate with other users that are in the same location and/or have the same interests.

Regarding Claim 12,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the authenticator resides in an edge device (Column 10, line 64 to Column 11, line 16).

Regarding Claim 13,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses an edge device for connecting a user station to a network switch (Figures 2-3).

Regarding Claim 14,

Stewart as modified by Torvinen discloses the system of claim 13, in addition, Stewart discloses that the edge device is a wireless access point (Column 10, line 64 to Column 11, line 16).

Regarding Claim 15,

Stewart as modified by Torvinen discloses the system of claim 14, in addition, Stewart discloses that the user is capable of connecting to the network through the access point (Column 5, lines 1-14; and Column 10, line 64 to Column 11, line 16).

Regarding Claim 16,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the client is a wired device capable of connecting to the network through an Ethernet port (Column 5, lines 2-24; Column 6, lines 40-59; and Column 9, lines 48-64).

Regarding Claim 18,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the location information indicates the location of an edge device for connecting the client to the network (Column 10, line 64 to Column 11, line 27).

Regarding Claim 19,

Stewart as modified by Torvinen discloses the system of claim 18, in addition, Torvinen discloses an interface for permitting an administrator to associate the location information to the edge device (Paragraph 40; associating a location-based group with edge devices, such as base stations).

Regarding Claim 21,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the authentication server authenticates the identity (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; Column 14, lines 40-56; Column 16, lines 38-55; and Column 18, lines 1-25).

Regarding Claim 22,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the authentication server includes a policy designating locations, if any, at which the client is permitted to connect to the network (Column 11, lines 28-53; and Column 16, lines 38-64); and Torvinen discloses that the authentication server (application server in some embodiments) includes a policy designating locations at which a client is permitted to connect to the network in order to access each group (Paragraph 42).

Regarding Claim 24,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the identity includes information selected from the group consisting of a user name, a user password, a certificate, a MAC address, a shared key, a smart card identifier, and any combination of the foregoing information (Column 10, lines 53-63).

11. Claims 11, 20, 27-29, and 31-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen, further in view of Kwan (U.S. Patent Application Publication 2004/0255154).

Regarding Claim 11,

Stewart as modified by Torvinen does not explicitly disclose that the authenticator resides in a network switch.

Kwan, however, discloses that the authenticator resides in a network switch (Paragraph 56). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the multi-tiered network security system of Kwan into the distributed network access system of Stewart as modified by Torvinen in order to ensure that a client and it's associated user are authentic and authorized to use the system by three levels of security checks, including physical address authentication of the device, user credential authentication, and VLAN group association checks, thereby increasing security of the system.

Regarding Claim 20,

Stewart as modified by Torvinen does not explicitly disclose that the authentication server is included in a network switch.

Kwan, however, discloses that the authentication server is included in a network switch (Paragraph 36). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the multi-tiered network security system of

Kwan into the distributed network access system of Stewart as modified by Torvinen in order to ensure that a client and it's associated user are authentic and authorized to use the system by three levels of security checks, including physical address authentication of the device, user credential authentication, and VLAN group association checks, thereby increasing security of the system.

Regarding Claim 27,

Stewart discloses a network system comprising:

A plurality of edge devices capable of communicating with a plurality of user stations over one or more wireless channels (Figure 1; and Column 10, line 64 to Column 11, line 16);

A network switch including a plurality of ports for connecting the edge devices to a network (Figures 2-3; and Column 9, lines 52-64);

An application for requesting station identities from the user stations and for associating corresponding location information with each of the station identities (Column 10, line 64 to Column 11, line 53);

A data structure, accessible by an authentication server, associating identities of clients with their authorized access locations (Column 7, line 24 to Column 8, line 3; and Column 12,

line 55 to Column 13, line 11; Column 15, lines 17-28; and Column 16, lines 38-55);

The authentication server deciding whether to grant or deny each of the user stations access to the network by accessing the data structure and determining, for each user station, that the location information corresponding to the user stations specifies a location that is one of the authorized access locations, if any, for the user station as maintained in the data structure (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; Column 14, lines 40-56; Column 16, lines 38-55; and Column 18, lines 1-25);

But does not explicitly disclose that the application is run on the network switch or a network manager, directly connected to the authentication server, that allows a network administrator to create and update the data structure.

Torvinen, however, discloses a network manager, directly connected to the authentication server, that allows a network administrator to create and update the data structure (Paragraphs 27-28, 42, 45, and 54; components on the server that store, access, modify, and validate group information regarding locations and group members). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the conditional group access system of Torvinen into the distributed network access system of Stewart in order to allow

various groups to be formed, by network operators and normal users alike, such that groups may be based upon the location of the device, device capabilities, user capabilities or subscriptions, etc., thereby providing additional beneficial services to users by allowing them to communicate with other users that are in the same location and/or have the same interests.

Kwan, however, discloses an application running on a network switch, for requesting station identities from user stations (Paragraph 56). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the multi-tiered network security system of Kwan into the distributed network access system of Stewart as modified by Torvinen in order to ensure that a client and it's associated user are authentic and authorized to use the system by three levels of security checks, including physical address authentication of the device, user credential authentication, and VLAN group association checks, thereby increasing security of the system.

Regarding Claim 28,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Stewart discloses that at least one of the edge devices is a wireless access point (Figure 1; and Column 10, line 64 to Column 11, line 16).

Regarding Claim 29,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Kwan discloses a user station that is a wired device for directly connecting to one of the ports of the network switch (Figure 1; and Paragraph 35).

Regarding Claim 31,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Stewart discloses that the location information indicates the location of one of the edge devices (Column 10, line 64 to Column 11, line 27).

Regarding Claim 32,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Torvinen discloses an interface for permitting an administrator to associate the location information to the edge devices (Paragraph 40); and Kwan discloses that the network switch includes an interface for permitting an administrator to set information (Figure 2, element 210; and Paragraph 30).

Regarding Claim 33,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Kwan discloses that the network switch includes an authenticator for authenticating the station identities (Paragraph 56).

Regarding Claim 34,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Stewart discloses that the authentication server authenticates the station identities (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; Column 14, lines 40-56; Column 16, lines 38-55; and Column 18, lines 1-25).

Regarding Claim 35,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Stewart discloses that the authentication server includes a policy designating locations, if any, at which the user stations are permitted to connect to the network (Column 11, lines 28-53; and Column 16, lines 38-64).

Regarding Claim 36,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Kwan discloses that the authentication server is a RADIUS server (Paragraphs 33 and 57).

Regarding Claim 37,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Stewart discloses that the station identities include information selected from the group consisting of a user name, a user password, a certificate, a MAC address, a shared key, a smart card identifier, and any combination of the foregoing information (Column 10, lines 53-65).

12. Claims 17 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen, further in view of Liming.

Regarding Claim 17,

Stewart as modified by Torvinen does not explicitly disclose that the location information indicates the location of a network switch to which the client is attempting to connect.

Liming, however, discloses that the location information indicates the location of a network switch to which the client is attempting to connect (Paragraph 159). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the location context system of Liming into the distributed network access system of Stewart as modified by Torvinen in order to allow the system to associate location information with the client even when the other devices cannot provide such location information, thereby extending the system to be able to be used when the client connects directly to a switch and/or when the other devices between the client and switch do not have any means to associate location information with the client.

Regarding Claim 49,

Stewart as modified by Torvinen and Liming discloses the system of claim 17, in addition, Liming discloses that the location information indicates the location of a port of a network switch to which the client is attempting to connect (Paragraph 159).

13. Claims 23, 25, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen, further in view of Funk.

Regarding Claim 23,

Stewart as modified by Torvinen does not explicitly disclose that the authentication server is a RADIUS server.

Funk, however, discloses that the authentication server is a RADIUS server (Pages 1-6). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Torvinen in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

Regarding Claim 25,

Stewart as modified by Torvinen does not explicitly disclose a network switch that comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

Funk, however, discloses a network switch that comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of

the foregoing (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Torvinen in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

Regarding Claim 26,

Stewart as modified by Torvinen does not explicitly disclose that the authentication server comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

Funk, however, discloses that the authentication server comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Torvinen in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest

of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

14. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen and Kwan, further in view of Liming.

Stewart as modified by Torvinen and Kwan does not explicitly disclose that the location information indicates the location of the network switch.

Liming, however, discloses that the location information indicates the location of the network switch (Paragraph 159). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the location context system of Liming into the distributed network access system of Stewart as modified by Torvinen and Kwan in order to allow the system to associate location information with the client even when the other devices cannot provide such location information, thereby extending the system to be able to be used when the client connects directly to a switch and/or when the other devices between the client and switch do not have any means to associate location information with the client.

15. Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen and Kwan, further in view of Funk.

Stewart as modified by Torvinen and Kwan does not explicitly disclose an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

Funk, however, discloses an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Torvinen and Kwan in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

16. Claim 50 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen, further in view of Tan (U.S. Patent Application Publication 2001/0045451).

Stewart as modified by Torvinen does not explicitly disclose that the identity includes a smart card identifier.

Tan, however, discloses that the identity includes a smart card identifier (Paragraphs 20-23). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate

the smart card-based authentication techniques of Tan into the distributed network access system of Stewart as modified by Torvinen in order to provide multiple factor authentication, such that the user must first authenticate to the smart card, which will then allow the smart card to authenticate with the authentication server in a much more secure manner than simply by sending a username and/or password to the server for authentication.

17. Claim 51 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen and Kwan, further in view of Tan.

Stewart as modified by Torvinen and Kwan does not explicitly disclose that the identity includes a smart card identifier.

Tan, however, discloses that the identity includes a smart card identifier (Paragraphs 20-23). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the smart card-based authentication techniques of Tan into the distributed network access system of Stewart as modified by Torvinen and Kwan in order to provide multiple factor authentication, such that the user must first authenticate to the smart card, which will then allow the smart card to authenticate with the authentication server in a much more secure manner than simply by sending a username and/or password to the server for authentication.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437